

Universidad Nacional Autónoma de México

Seguridad Electrónica

Grupo: 2257

García Solórzano Paris Roberto

Gonzales Canseco Ricardo Emanuel

Pérez Ruíz Hugo Alberto



Eficiencia de la Seguridad electrónica usada en México

Diagrama matricial

Problema	Objetivos	Pregunta	Hipótesis
¿Qué tan eficiente es la seguridad electrónica usada en México?	Saber cuántas cuentas o sistemas son hackeadas	¿Cuántas veces es usada o vista información sin consentimiento?	En México no hay tecnología de punta y si bastantes hacker, es posible que varias veces.
	Saber los parámetros a nivel mundial	¿Cuántas veces se vulnera la seguridad electrónica a nivel mundial?	es posible que México esté por debajo del promedio
	Enterarse de que se puede hacer para mejorar la eficiencia	¿Qué podría mejorar la eficiencia de la S.E.?	

¿Qué es la Seguridad Electrónica?

Que es seguridad Electrónica? Esta parte de la seguridad es vista como el área que presta herramientas de última tecnología para ayudar a completar las otras áreas de seguridad. En esta área se puede encontrar tanto como usted necesite, ya que hay desde un simple controlador eléctrico para picaportes que se pone en una puerta con un pulsador cualquiera, hasta un scanner ocular para control de retina color y forma de un ojo. Es importante mencionar que el mercado de seguridad es muy grande en el mundo, por lo que en tecnología no se queda atrás y las opciones están para que usted; acorde a su presupuesto, se ayude de ellas para estar bien protegido.

- 2. Los Sistemas de Seguridad Electrónica. En la implementación de sistemas integrales de seguridad financiera, la seguridad electrónica es el complemento natural de la seguridad física. La importancia de los Sistemas de Seguridad Electrónica, radica en que se sustenta en el uso de alta tecnología aplicada a la seguridad y soportada en un adecuado diseño, instalación e interconexión, de modo tal, que permita obtener una alerta temprana de los eventos generados en las instalaciones, en el momento en que están siendo vulneradas por personas no ajenas a la organización. De igual modo para los sistemas de Circuito Cerrado de Televisión (CCTV), su importancia está dada por la funcionalidad del registro de imágenes en el momento en el que ocurren los acontecimientos, ya sea en medios magnéticos u ópticos, los cuales pueden ser consultados en el momento en el que se producen, o posteriormente para identificar con mayor detalle lo que se desee sobre las imágenes grabadas por estos sistemas, apoyados en equipos informáticos.
- 3. Que se puede encontrar Alarmas CCTV y Accesorios Controladores de picaportes para puertas Dispositivos de alto voltaje Seguridad Perimetral Localizadores satelitales, y de frecuencia Dispositivos Personales Sensores de Movimiento Controles de Acceso Comunicación de una y de doble vía.

- 4. A la Seguridad Electrónica hay que tomarla como un recurso que existe para utilizarlo siempre que se esté haciendo un programa de aseguramiento de un área o persona específica, ya que sus alternativas son tantas que mencionarlas sin saber el lugar y el presupuesto se torna un tanto falaz, por lo que esté seguro que en una asesoría de Asseguri utilizaremos esta herramienta para que usted esté bien protegido. Recuerde que Asseguri no vende, por lo que la asesoría será la real para su caso específico.
- 5. Porque es importante la Seguridad Electrónica? Los criterios que fundamentan el porqué es importante y necesaria la implementación de "Sistemas de Seguridad Electrónica", son los siguientes: . Siempre existen actividades no previstas, y si lo están, siempre se presentan imprevistos: Desde una remodelación de instalaciones efectuado por personal que no necesariamente conoce de sistemas de seguridad, condiciones climáticas variables o extremas que pueden alterar el correcto funcionamiento de los equipos y dispositivos, hasta sabotajes e intentos de intrusión. 2. Son nuestros ojos y oídos las 24 horas del día, los 7 días de la semana: La tecnología ha logrado un gran desarrollo, permitiendo contar en la actualidad con equipos y dispositivos de seguridad confiables, facilitando la tarea de control y supervisión, manteniéndonos informados de lo que ocurre en nuestras instalaciones aún cuando no estemos presentes

¿Qué podría hacerse para mejorar la S.E.?

- Un diseño adecuado es indispensable: Toda la tecnología disponible no sirve por más sofisticada que sea, si el diseño del sistema de seguridad que ha de ser implementado en sus instalaciones, no cuenta con un respaldo de conocimientos y experiencia probada y comprobada; esto solo puede ser ofrecido por empresas especializadas que demuestren que cuenta con el personal calificado y la experticia necesaria, para garantizar el correcto funcionamiento del diseño ofrecido. 4. Debe existir una periodicidad para ejecutar el mantenimiento preventivo: Recuerde que es como un seguro, ya que si le falla cuando usted más lo necesita de nada valdrá haber invertido en instalarlo para asegurar sus instalaciones, determinándose su periodicidad en función al tipo de sistema de alarma instalado, y otras condiciones particulares que se determinen para cada sistema.
- 7. 5. Familiarícese con su sistema de alarma: Recuerde que cuanto mayor sea el conocimiento de sus sistemas de alarma por parte de los funcionarios y empleados a cargo de la seguridad interna de su entidad, mayor será el provecho que puede obtener del mismo, adoptando actitudes pro activas en beneficio de la seguridad de sus instalaciones. 6. Confianza y Seguridad: Son los dos principales pilares que sustentan el normal desarrollo y la continuidad del negocio financiero en nuestro país, por tal motivo, se debe considerar que el mantenimiento de los sistemas de seguridad electrónica debe ser efectuado por una entidad que contribuya a cumplir con estos objetivos.

Aplicación del método de Porter En la venta de seguridad electrónica

- Barreras que podrían crear los competidores existentes:

Costo elevado de investigación

Clientes cambian pocas veces su sistema de seguridad

El costo para financiar el negocio no es exageradamente caro, pero si considerablemente

Costo de capacitación de los empleados elevado, pues hay que ir al día con la tecnología

- Factores que pueden incrementar la rivalidad con otras empresas
- Hay pocos competidores, pero casi todos en las mismas condiciones y posibilidades
- Los clientes no ven fácilmente la diferencia entre los distintos productos, por tratarse de tecnología
- Alta variación de precios
- Las empresas de este sector solo se dedican a este tipo de tecnología y difícilmente salen del sector
- Presión de productos sustitutos
- Lo que ofrece cada empresa de seguridad electrónica tiene varios sustitutos muy parecidos en función y calidad, la diferencia puede llegar a ser el precio, desestabilizando estos últimos.
- Poder de negociación que ejercen los proveedores
- Por el momento sigue siendo poco el material de trabajo de los sistemas de seguridad (chips, dispositivos, etc.), y contados los proveedores.
- Las mismas empresas de seguridad electrónica pueden crear su demás material de trabajo a nivel software
- Poder de negociación de los compradores
- Las compras representan una parte significativa de los ingresos anuales, pues se les vende a pocos.
- Si el cliente desea cambiar de proveedor, esto no le representa un gasto grande
- Existen productos similares.

Vistazo al mercado de la seguridad electrónica.

Un tema tan sensible como la Seguridad demanda la participación de todos sus actores; en México y el resto de Latinoamérica es una preocupación constante que genera opciones en materia de negocios, tal es el caso de la seguridad física electrónica que se suma al crecimiento de la economía en su conjunto.

De acuerdo con el estudio de Asociación de la Industria de la Seguridad (SIA), el mercado de la EPS (Electric Power Steering- por sus siglas en inglés) en los seis países latinoamericanos estudiados durante 2008 reportó el valor del mercado en 704 millones de dólares distribuidos de la siguiente forma: Chile 6%; Venezuela 8% Venezuela 8%, Colombia Colombia 110% Argentina Argentina 12%, México 61% y Panamá 3%.

Seguramente los actores involucrados en la industria de la seguridad electrónica lo saben y están enterados del referido análisis que da cuenta de la demanda de productos de seguridad en dichos países reflejando un alto crecimiento de este mercado en productos de seguridad.

Los sistemas de video representan el mayor segmento del mercado de seguridad física en las seis naciones antes citadas con un tamaño de mercado de 263 millones de dólares. La alarma de intrusión de sistemas está en segunda posición con 124 millones. Los ingresos provienen de las no-residenciales del mercado.

Ejemplo de una empresa de Seguridad Electrónica

INSERTEC, S.A

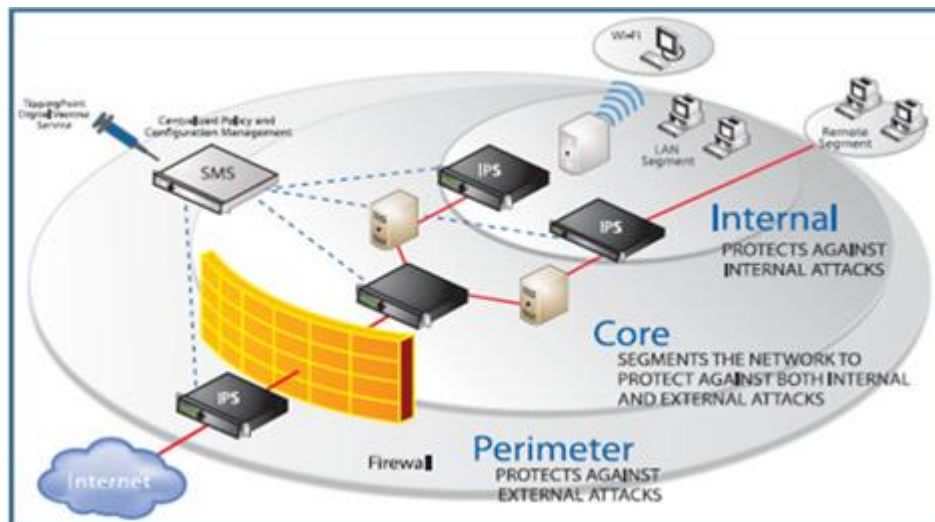
Hablar de seguridad siempre ha sido hablar de una amplia serie de pasos y equipos de red que interactúan sobre la información que circula en las redes de datos y que requieren de varios pasos de administración y configuración para poder garantizar que la información que es transportada por la red sea mantenga segura; que sea información válida y debidamente autorizada, y que se transporte con la velocidad óptima hacia su destino final. Por tanto la necesidad de añadir políticas de seguridad a las redes de datos se ha vuelto una inminente necesidad, pues en el mundo de las redes convergentes, redes en la que circulan datos, voz y video y accesos a Internet, el mantener la red interna a salvo de cualquier vulnerabilidad es un tema de gran importancia para quienes las administran.

Para lograr este fin, la industria de las telecomunicaciones ofrece actualmente una serie de productos que son capaces de brindar las tecnologías apropiadas para el eficiente manejo de los paquetes de información que viajan por las redes de datos. Entre estas tecnologías se encuentran las siguientes:

- QoS (Quality of Service): Conjunto de protocolos o mecanismos de manejo de paquetes que asegura la integridad y prioridad de un paquete al viajar por la red de datos.
- Filtrado de Contenido: Capacidad del producto de inspeccionar y validar cierta clase de información y contenido que los paquetes lleven consigo.
- Limitación de ancho de banda (Rate-Limit): Capacidad del producto de limitar el ancho de banda ó cantidad de recursos de red que algún tipo de tráfico esté utilizando, de tal forma de garantizar la mayor disponibilidad de los recursos de la red para el tráfico de mayor prioridad dentro de la misma.

Todo lo anterior muestra que, cuando hablamos de seguridad de redes, no solo estamos hablando de la capacidad de contar con tecnologías que permitan proteger la red de virus, de software espía, de ataques de negación de servicio y otros, sino que también, por SEGURIDAD de todo el tráfico válido y autorizado que circula por la red, estas tecnologías permitan el mejor y más óptimo desempeño de todos y cada uno de los servicios de red para los cuales esta fue implementada. En la siguiente gráfica se muestra un ejemplo de implementación de seguridad de red a partir de poner en sitios estratégicos de la red, un sistema de pro-activo de

prevención de intrusos IPS 3Com TippingPoint (IPS por sus siglas en inglés).



ISERTEC en el mundo de la seguridad de redes

3Com tiene una división que es líder en el amplio mundo de la seguridad de valor agregado de redes, y esta división cuenta con su plataforma de seguridad llamada TippingPoint. Este producto es un IPS, un sistema pro-activo de detección de intrusos, que más allá de detectar intrusos en la red, es capaz de detener la actuación de este intruso en la red. Además es capaz de identificar cualquier tipo de tráfico en la red que no sea válido y que no esté autorizado y detenerlo o aislarlo, protegiendo así el rendimiento de la red.

Esta robusta plataforma de inspección constante del tráfico de red está basada en un robusto hardware de circuitos integrados de alta velocidad de procesamiento, lo cual lo hace la solución de más alto desempeño y rendimiento en el análisis de paquetes por segundo en la industria. Estos productos tienen la capacidad de proveer un completo portafolio de opciones de equipo que se ajustan a las necesidades de cada empresa, pues TippingPoint cuenta con modelos de equipos capaces de analizar desde 50 MB de tráfico efectivo de paquetes por segundo hasta equipos capaces de analizar 5 GB de tráfico efectivo circulando a través de ellos.

Debido a contar con sólido equipo de ingenieros que constantemente están monitoreando el comportamiento de tráfico anómalo; vulnerabilidades de sistemas operativos de computadoras que pueden ser presa fácil de virus ó vulnerabilidades que un hacker puede explotar para usos ilícitos; la división de seguridad de 3Com, TippingPoint, garantiza a sus cliente tener las políticas de filtrado de tráfico siempre actualizadas para poder así, garantizar la protección de la red de datos en donde cada equipo IPS se encuentre instalado. A continuación, los diferentes modelos de IPS que la división de seguridad de 3Com, TippingPoint, pone al alcance de sus clientes.

Fuente.

<http://www.infochannel.com.mx>

<http://www.isertec.com/> -seguridad-electrónica

<http://www.slideshare.net/martinn2/que-es-seguridad-electrnica>